

Purchase and Import a Signed SSL Certificate

Copyright© 2015 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

1

Overview

STEP 1: Purchase an SSL certificate package from a Certificate Authority (CA)

STEP 2: Generate a Certificate Signing Request (CSR)

STEP 3: Setup the SSL certificate

STEP 4: Import the signed certificate into your FortiGate device

STEP 5: Configure your FortiGate device to use the signed certificate

2

Detailed Steps



Before creating a certificate, you must have a registered domain.

STEP 1: Purchase an SSL certificate package from a Certificate Authority (CA)

SSL certificate packages can be purchased from any CA, such as [Comodo](#), [GoDaddy](#), or [GlobalSign](#).

To purchase a certificate package:

1. Create an account with your chosen vendor, or use the account you used to purchase your domain.
2. Locate the SSL Certificates page.
3. Purchase a basic SSL certificate for domain validation only.



If required, a more secure SSL certificate can be purchased.

After purchasing the certificate, the CA will direct you to setup the certificate so that it can be verified.

If you need to create a CSR, go to STEP 2.

If not, skip to STEP 3.

STEP 2: Generate a Certificate Signing Request (CSR)

Some CAs can auto-generate the CSR during the signing process, or provide tools for creating CSRs, such as GlobalSign's [SSL Certificate Signing Request Tool](#).

If necessary, a CSR can be quickly created from your FortiGate device's GUI.

1. Log in to your FortiGate unit and browse to *System > Certificates*.
2. Select *Generate* in the toolbar.

The screenshot shows the 'Generate Certificate Signing Request' form. It has a title bar 'Generate Certificate Signing Request'. Below it, the 'Certificate Name' field is filled with 'fortisslvpndemo'. The 'Subject Information' section includes 'ID Type' set to 'Domain Name' and 'Domain Name' filled with 'fortisslvpndemo.com'. The 'Optional Information' section has fields for 'Organization Unit', 'Organization', 'Locality(City)', 'State/Province', 'Country/Region' (a dropdown menu), 'E-mail' filled with 'fortisslvpndemo@fortinet.com', and 'Subject Alternative Name'. The 'Key Type' is set to 'RSA' and 'Key Size' is set to '2048 Bit'. The 'Enrollment Method' has 'File Based' selected with a radio button. At the bottom are 'OK' and 'Cancel' buttons.

3. Enter the required information in the *Generate Certificate Signing Request* screen:
 - Ensure that the certificate has a unique name.
 - Select *Domain Name* in the *ID Type* field.
 - An email address is required.
 - Ensure that the *Key Size* is set to *2048 Bit*.
 - Set the *Enrollment Method* to *File Based*.

4. Select *OK* to create the CSR.

The CSR will be added to the certificate list with a status of *PENDING*.

5. Select the new CSR in the *Local Certificates* page and select *Download* to save the CSR to your computer.

The CSR file can be opened in any text editor and should resemble the following:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDDjCCAFYCAQAwgZcx CzAJBgNVBAYTA1VTMREwDwYDVQQIEWhOZXcgWW9ya zEV
MBMGA1UEBxMMTMV3IE5ldyBZb3JrMRcwFQYDVQQKEw5QbGFuZlZlZlZlZlZlZlZl
MAsGA1UECxmEQ3JldzEQMA4GA1UEAxMHMC4wLjAuMDEkMCIIGCSqSgIb3DQEJARYV
ZnJ5QHBsYW5ldGV4cHJlc3MuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAr8yFQ7lmm0MS15zrAP174HDIrUwVzKNmhYQdGVdM6g+ikOmLM7arStXX
4znafar9IPI/ugAxXdXRy/w6tTzH8W8Ds jnrW0EGwXHnujpPNvnsEqtPO5fezje4
lQKJbLlNVUdzM3Finhd+28xPwLkAiL+5rLnTA5zB8onf3R98+PdE+R57xRwawHSr
XhJMSRbpl7IDHW23IL6Vet9FB5bSFQIS5yjs1J8JHcnW+oxnNwngdi1219XI/Kbb
NRrh2QT6S+Ntftz0ZkGVX6fJOY4b+JCa4op41J4Jp6yoZUbkpVeBtXgrz2n6ulwKw
HjKRokWM5SG16haFyM3V+ExUFxbiAwIDAQABODEwEQYDVIR0TMQoTCENBokZBTfNF
MBwGCSqSgIb3DQEJJDjEPMA0wCwYDVIR0PBAQDAgWgMA0GCSqSgIb3DQEBcWUAA4IB
AQCT+f07oMvDDDI ZMKZskInGgCpN1DRELiRgyj0d5Xt3lby78G2N15++vfe/Tsdu
dBrRdA6eAyVgEhBk76JiVUpluQ9dm3TRDpZp/bc+kHc8712NVSZEpjAKaAeOx5E
0GwGqQKk1RtX00ABA2b6WxK9azg/TdHS5ZTMm+jCl6xacgJ8qCt9N12DL1WHaXy8
ZO/jI00vpX9FgKVL Rq7glpmZgsA7bcZu+NitN0JbARyUL8038URFEiqXzTuR7vX5
LwvNhqqJ9obGAHyFLxn/BsOQA0LQ9jnhWpVasDj3NUS3V6j3+31db921Dp10kbbHH
WP2WDWfUp8zx1jYQJpgOjBmW
-----END CERTIFICATE REQUEST-----
```


STEP 3: Setup the SSL certificate



The following instruction use GoDaddy as an example.

1. Immediately after purchasing the certificate, you will be taken to your account page.
2. Find the newly purchased certificate and select *Manage* to open the *Certificate* page.
3. Select *Setup*.
4. If you are using a CSR generated by your FortiGate device:
 - a. Open the CSR file in a text editor
 - b. Copy the file contents
 - c. Paste it into the text box.
5. Select a signature algorithm, read and then agree to the subscriber agreement, then select *Request Certificate*.

1 Year Standard SSL Certificate Certificate Setup

Choose website

The screenshot shows the 'Provide a certificate signing request (CSR)' form on the GoDaddy website. It includes a text area for the CSR content, a domain name field, a signature algorithm dropdown, and a checkbox for agreeing to the terms and conditions.

Provide a certificate signing request (CSR)

Certificate Signing Request (CSR) [Learn more](#)

```
/YYPodYhC4mDd4JULhzmwQ10ppRLXAVAJINL0rkDXGjN0pnaxDI  
rjdR2Pi0EzTgbr8MF7NqceVO2QziPFrsOy0=  
-----END CERTIFICATE REQUEST-----
```

Domain Name (based on CSR):
demo.fortinet.com

[Hide advanced options](#)

Signature Algorithm [Learn more](#)
GoDaddy SHA-2

☒ I agree to the terms and conditions of the [Subscriber Agreement](#).

[Request Certificate](#) [Cancel](#)

6. The *Certificate Verification* screen opens, the certificate is verified, and you are redirected to the *Certificate Management* screen.
7. Select *Download* to download the signed certificate, as a Zip file, to your computer.
The server type can be set to *Other*.

STEP 4: Import the signed certificate into your FortiGate device

1. Unzip the file downloaded from the CA.

There should be two .CRT files: a CA certificate with *bundle* in the file name, and a local certificate.

2. Log in to your FortiGate unit and browse to *System > Certificates*.
3. Select *Import > Local Certificate* to import the local certificate.

Name	Subject	Comments	Issuer	Expires	Status	Ref.
Local CA Certificates (1)						
Fortinet_CA_SSLProxy	C = US, CN = FortiGate CA, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = Certificate Authority	This is the default CA certifi...	Fortinet	2028-10-13 00:46:39 GMT	OK	13
Certificates (4)						
Fortinet_Factory	C = US, CH = PG200P3911800062, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = FortiGate	This certificate is embedded in...	Fortinet	2038-01-19 03:14:07 GMT	OK	1
Fortinet_Firmware	C = US, CN = FortiGate, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = FortiGate	This certificate is embedded in...	Fortinet	2038-01-19 03:14:07 GMT	OK	1
Fortinet_SSLProxy	C = US, CH = FortiGate Server, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = FortiGate		Fortinet	2024-02-26 22:59:21 GMT	OK	26
Fortinet_WiFi	OU = PositiveSSL, CN = auth-cert.fortinet.com	This certificate is embedded in...	Comodo CA Limited	2020-09-21 23:59:59 GMT	OK	1
External CA Certificates (2)						
Fortinet_CA	C = US, CN = support, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = Certificate Authority		Fortinet	2038-01-19 03:14:07 GMT	OK	0
PositiveSSL_CA	CN = PositiveSSL, CA, C = GB, L = Salford, O = Comodo CA Limited, ST = Greater Manchester		The USERTRUST Network	2020-05-30 10:48:38 GMT	OK	1

The status of the certificate will change from *PENDING* to *OK*.

4. Import the CA certificate by selecting *Import > CA Certificate*. It will be listed in the *CA Certificates* section of the certificates list.

You can now configure SSL VPN using the signed certificate.

STEP 5: Configure your FortiGate device to use the signed certificate

- 1. Log in to your FortiGate unit and browse to *VPN > SSL > Settings*.
- 2. In the *Connection Settings* section, locate the *Server Certificate* field.

SSL-VPN Settings

Connection Settings

Define how users can connect and interact with SSL-VPN portals on this FortiGate.

Listen on Interface(s)

Click to set...

This is generally your external interface (i.e. wan1)

Listen on Port

1985

Restrict Access

☐ Allow access from any host

☒ Limit access to specific hosts

Click to add...

Idle Logout

☒ Logout users when inactive for specified period

☐ Never logout inactive users

Inactive For

25

(Seconds)

Server Certificate

DemoCert

Require Client Certificate

Please Select

Tunnel Mode Client Settings

Once connected in tunnel mode

Address Range

Specify custom IP ranges of 10.212.134.200 - 10.212.134.210

DNS Server

Specify

Specify WINS Servers

Allow Endpoint Registration

☐

Fortinet_CA_SSLProxy

Fortinet_Factory

Fortinet_Factory2

Fortinet_Firmware

Fortinet_SSLProxy

Fortinet_Wifi

Authentication/Portal Mapping

By default, all users see the same SSL-VPN portal. The following table allows you to assign different portals to different users and groups.

Create New

Edit

Delete

Users/Groups	Portal
All Other Users/Groups	Not Set

Apply

- 3. Select the new certificate from the drop-down menu.
- 4. Select *Apply* to configure SSL VPN to use the new certificate.

For more information on configuring SSL VPN, see the [SSL VPN Guide](#), available in the [Fortinet Document Library](#) or watch the video available in the [Fortinet Video Library](#).

FORTINET.